Dirk Dekker
Van Uytrechtlaan 25
1901 JK Castricum
T.J.Dekker@uva.nl.

# Priemgetallen en priemidealen in kwadratische lichamen

## 1. Inleiding

Het ontbinden van getallen in factoren en de daaruit te verkrijgen ondeelbare factoren – priemgetallen – hebben sinds de oudheid veel belangstelling van wiskundigen gehad.
Met name de onregelmatige verdeling van priemgetallen is fascinerend, en in de moderne tijd vindt ontbinding van grote getallen toepassing in de cryptografie voor het beveiligen van geheime berichten. Voor een aardig overzicht zie het boek 'De pracht van priemgetallen' door Levrie & Penne (2014).

In plaats van gehele getallen, kunnen we ook uitgebreidere getalsystemen beschouwen, met name ringen en lichamen van algebraische getallen. Deze zijn vooral sinds de 19$^{e}$ eeuw uitvoerig bestudeerd. Er is dan ook veel over bekend, onder meer aangaande het ontbinden in factoren en eigenschappen van priemgetallen.

In het bijzonder beschouwen we - als eenvoudigste systemen - ringen en lichamen van kwadratische getallen. Deze zijn op natuurlijke wijze in het platte vlak voor te stellen.
De priemgetallen hierin vormen fraaie patronen. Doel van dit artikel is, na een beknopte beschrijving van de theorie, algoritmen te presenteren die plaatjes van deze patronen leveren en een indruk te geven van diverse patronen voor verschillende ringen.

We geven hier de benodigde theorie slechts summier. Voor meer informatie zie bijvoorbeeld Lejeune Dirichlet / Dedekind (1893), Borewicz & Safarevic (1966), Ireland & Rosen (1982), Cohen (1993) en eerdere publicaties van mijn hand: Dekker (1994 & 2010).

## 2. Lichamen en ringen van algebraische getallen

De *algebraische getallen* zijn nulpunten van polynomen met gehele coëfficiënten.
Ze heten *gehele algebraische* getallen als de voorste coëfficiënt ervan gelijk aan 1 is.
Een *algebraisch getallenlichaam* is een uitbreiding van het lichaam Q der rationale getallen verkregen door toevoeging van een (niet-rationaal) algebraisch getal. Zij $\alpha$ zo'n algebraïsch getal, dan is $Q(\alpha)$ het kleinste lichaam dat Q en $\alpha$ omvat. De gehele algebraische getallen hierin vormen een ring D (integriteitsgebied, *domain of integers*).

kwadratische getallen
Een eenvoudig systeem van algebraische getallen wordt verkregen door aan het lichaam Q der rationale getallen een kwadratisch getal $\sqrt{r}$ toe te voegen, waarbij de *radicand* r geheel maar geen kwadraat is, en tevens *kwadraat-vrij*, d.w.z. dat r geen kwadraat van een priem-getal als factor bevat. Dit systeem, het *kwadratische lichaam* $Q(\sqrt{r})$, bestaat uit de getallen

$$x + y\sqrt{r},$$

waarbij x en y rationaal zijn. Elk element hiervan is wortel van een kwadratische vergelijking met gehele coefficienten. De gehele algebraische getallen in $Q(\sqrt{r})$ vormen een ring D.

Deze bestaat uit de getallen $x + y \sqrt{r}$ waarbij x en y geheel zijn als r een 4-voud plus 2 of 3 is. Anders is r een 4-voud plus 1 en zijn de getallen $x + y \sqrt{r}$ geheel algebraisch niet alleen voor gehele x en y, maar ook wanneer x en y beide gehele getallen plus 1/2 zijn. D wordt dus voortgebracht door *voortbrengende* $\tau = \sqrt{r}$ als r een 4-voud plus 2 of 3 is, anders $\tau = (1+\sqrt{r})/2$. De ring D wordt wel aangeduid als $Z[\tau]$. Aldus kan $Z[\sqrt{r}]$ worden voorgesteld in een vlak vierkant rooster en $Z[(1+\sqrt{r})/2]$ in een vlak driehoekig rooster, waarin opvolgende rijen - met constante y-waarde – telkens een halve positie opschuiven.

De discriminant d van de vierkants-vergelijking die de voortbrengende als wortel heeft, heet tevens *discriminant van de ring* en speelt een belangrijke rol in de theorie. Hiervoor geldt, als r een 4-voud plus 2 of 3 is, $d = 4r$ en anders is r een 4-voud plus 1 en $d = r$. En de formule voor de voortbrengende $\tau$ kan dan worden samengevat als $\tau = (d \bmod 4 + \sqrt{d})/2$.

**3. Priemgetallen en ondeelbare getallen**

Een getal in de ring van algebraïsch gehelen in $Q(\alpha)$ is ofwel *eenheid*, dat is een getal waarvan het omgekeerde ook tot de ring behoort, of *samengesteld*, dat is product van minstens twee factoren die geen eenheden zijn, of anders *ondeelbaar*.

In de ring *geldt eenduidige factorisatie* als elk getal op slechts één manier is te ontbinden in ondeelbare factoren afgezien van eenheden en volgorde der factoren, d.w.z. twee ontbindingen van een getal hebben gelijk aantal ondeelbare factoren die zo in volgorde zijn te zetten dat elke factor gelijk is aan een eenheid maal de overeenkomstige factor.
Zulke ringen worden ook *Unique Factorization Domains* (UFD) genoemd.

Een *priemgetal* is een ondeelbaar getal dat, wanneer het deler is van een product van twee getallen, het altijd ook deler is van de ene of de andere factor ervan.

Als in een ring eenduidige factorisatie geldt, dan is elk ondeelbaar getal priemgetal en zijn deze twee begrippen dus gelijk. Als de eenduidige factorisatie niet geldt, dan is niet elk ondeelbaar getal een priemgetal.

<u>Voorbeeld</u>
In de ring $Z[\sqrt{-6}]$ geldt: $6 = 2 \times 3 = -\sqrt{-6} \times \sqrt{-6}$, en alle genoemde factoren zijn ondeelbaar, maar geen priemgetallen.

<u>kwadratische getallen</u>
Om te bepalen of een getal priemgetal is of niet, hoeven we alleen maar naar de norm ervan te kijken. In een kwadratisch getallenlichaam is deze gelijk aan het getal maal zijn toegevoegde waarde, waarbij we – voor de eenvoud – de absolute waarde nemen:

$$N(x + y \sqrt{r}) := |(x + y \sqrt{r})(x - y \sqrt{r})| = |x^2 - r y^2|.$$

Deze norm is altijd geheel, ook als r een 4-voud plus 1 is en x en y beide geheel plus 1/2. Verder geldt blijkbaar dat de norm van het product van twee getallen gelijk is aan het product van hun normen. Bovendien is de norm van eenheden gelijk aan 1.

De norm van een priemgetal in een kwadratische ring is ofwel zelf een priemgetal, p, of het kwadraat van een priemgetal, $p^2$. Is de norm gelijk aan p, dan is het getal vanzelfsprekend een priemgetal in de ring. Is de norm gelijk aan $p^2$, dan is het getal ofwel het product van twee

priemgetallen die elk norm gelijk aan p hebben, ofwel het getal zelf is een priemgetal in de ring (en is dan gelijk aan een eenheid maal p).
Dit hangt – voor oneven priem p - er van af of de discriminant (of de radicand, komt in dit geval op hetzelfde neer) van de ring een kwadraat is modulo p of niet. Zo ja, dan is het getal samengesteld uit twee factoren met norm p, anders is het getal een priemgetal in de ring.
Voor p = 2 geldt een afwijkend criterium: als de discriminant d een kwadraat is modulo 8, dus een 4-voud of een 8-voud plus 1, dan is het getal samengesteld, anders is d een 8-voud plus 5 en is het getal een priemgetal in de ring. (Is in het bijzonder p deler van d, dan is de ene factor van het getal een eenheid maal de andere factor.)

Dit alles geldt merendeels ook voor ringen die geen eenduidige factorisatie hebben. Alleen kan het dan voorkomen dat het getal in kwestie niet samengesteld is uit twee factoren, maar ondeelbaar (doch geen priemgetal) blijkt te zijn.

Voorbeelden
In de ring Z[√-1] is 2+√-1 priem want norm 5 is priem; 3 is priem want r = -1 is geen kwadraat modulo 3, maar 5 is niet priem want r = –1 is kwadraat modulo 5 en 2 ook niet, want d = –4 is 4-voud; er geldt: 5 = (2+√-1)(2-√-1), 2 = (1+√-1)(1-√-1).
In de ring Z[√-6] is 1+√-6 een priemgetal want norm 7 is priem; ook 13 is een priemgetal want r = -6 is geen kwadraat modulo 13; maar 2, 3 en 7 zijn geen priemgetallen; 7 is product van twee priemfactoren, 7 = (1+√-6)(1-√-6), en 2 en 3 zijn ondeelbaar, maar niet priem.

Eenduidige factorisatie
Er zijn onder de kwadratische ringen eindig veel complexe UFD (r < 0) – zie Stark (1967) – en vermoedelijk oneindig veel reële UFD (r > 0).
We geven een tabel van alle negen complexe en de reële tot r < 50.

| r mod 4 | complexe UFD, r < 0 | reële UFD, 0 < r < 45 |
|---|---|---|
| 1 | -3 -7 -11 -19 -43 -67 –163 | 5 13 17 21 29 33 37 41 |
| 2 of 3 | -1 -2 | 2 3 6 7 11 14 19 22 23 31 38 43 |

## 4. Idealen en priemidealen

Voor ringen zonder eenduidige factorisatie gaan we verder niet in op de bepaling van ondeelbare niet-priemgetallen. Voor deze ringen is, vooral in de 19$^{e}$ eeuw, een mooie theorie ontwikkeld, waardoor resultaten voor UFD op een bepaalde wijze tot niet-UFD zijn uit te breiden. Deze theorie betreft idealen.

Zij D de ring van algebraïsch gehelen in Q($\alpha$). Een ideaal A in D is een deelring in D met de eigenschap dat alle producten van elementen van D met elementen van A ook tot A behoren. Eenvoudigste voorbeelden zijn de hoofdidealen, dat zijn idealen voortgebracht door een enkel element van D; ze worden aangeduid door een voortbrengend element tussen haken.

Voorbeeld.
In de ring Z[√r] bestaan de idealen (3) en (2+√r) uit de getallen 3x+3y√r en (2+√r)(x+y√r).

Bijzondere idealen zijn het nulideaal (0) dat alleen 0 bevat, en het eenheidsideaal (1) dat gelijk is aan de hele ring D.
Het product AB van idealen A en B is het kleinste ideaal dat alle producten van elementen van A met elementen van B bevat.

Dit product is gelegen zowel in A als in B. Het omgekeerde geldt ook: als C een ideaal is gelegen in A, dan is A deler van C, d.w.z. er is een ideaal X zo dat C = AX.

Een priemideaal is een ideaal P in D, ongelijk aan het nul-ideaal en het eenheidsideaal D, zo dat, wanneer P deler is van het product AB van twee idealen, het deler is van A of van B. In het bijzonder geldt dat een hoofdideaal voortgebracht door een priemgetal een priemideaal is.

Voor idealen in D geldt de belangrijke stelling van Dedekind (1893):

> *Ieder niet-nul ideaal in D is eenduidig te schrijven als product van priemidealen, d.w.z. twee ontbindingen van eenzelfde ideaal hebben gelijk aantal priemidealen als factoren, die zo in volgorde zijn te plaatsen dat overeenkomstige factoren gelijk zijn.*

Een ideaal A in D verdeelt D in restklassen, waarbij per definitie twee elementen van D tot dezelfde restklasse behoren als hun verschil in A zit.
Als A niet het nulideaal is, dan is het aantal restklassen eindig. Dit aantal wordt per definitie de *norm* van het ideaal genoemd, en de norm van (0) is 0.
Dit komt goed uit, want als A een hoofdideaal is, dan is de norm van A gelijk aan de norm van een voortbrengende van A, zoals voor kwadratische lichamen boven is gedefinieerd.

Voorbeeld.
In de ring Z[√-6] is (√-6) een hoofdideaal met norm 6 en het ideaal voortgebracht door 2 en √-6 is een nevenideaal met norm 2, notatie (2, √-6).

De norm van het product van idealen is gelijk aan het product van hun normen.
De norm van een priemideaal is gelijk aan een macht van een priemgetal.

Is een ring geen UFD, dan zijn er naast hoofdidealen ook nevenidealen. In het bijzonder in een kwadratische ring wordt een nevenideaal voortgebracht door precies twee elementen.

kwadratische getallen
In een kwadratische ring kunnen de priemidealen worden bepaald door naar de norm van de idealen te kijken. De norm van een priemideaal is ofwel een priemgetal ofwel het kwadraat van een priemgetal. Is de norm een priemgetal p, dan is het ideaal een priemideaal. Is de norm het kwadraat $p^2$ van een priemgetal, dan hangt het van p en van de discriminant d van de ring af of het ideaal priem is of niet. Het criterium hiervoor is hetzelfde als boven beschreven voor het al of niet priem zijn van getallen in de ring en luidt dus als volgt.

Als d voor oneven p een kwadraat is modulo p, en voor p = 2 een kwadraat modulo 8, dus of een 4-voud of een 8-voud plus 1, dan is het hoofdideaal (p) product van twee priemidealen met norm p, anders is (p) een priemideaal in de ring.
(Is in het bijzonder p deler van d, dan is (p) product van twee gelijke priemidealen.)

## 5. Kwadratisch karakter

Het criterium welke idealen in een kwadratische ring met discriminant d (welke algebraische getallen in een kwadratisch UFD) priem zijn en welke niet, kan goed worden beschreven door middel van het karakter van de ring. Het *karakter* (engels: *character*) $\chi(x) = \chi(d, x)$ is een functie die aan elk niet-negatief geheel getal x een der waarden –1, 0, 1 toevoegt, en als volgt gedefinieerd is:

0. x en d hebben een priemfactor gemeen, dan: $\chi$ (d, x) = 0;

1. x = p is een oneven priemgetal dat geen factor van d is, dan:
$\chi$ (d, x) = 1 als d een kwadraat modulo p is, anders $\chi$ (d, x) = –1;

2. x = 2 en d is oneven dus een 4-voud plus 1, dan: $\chi$ (d, x) = 1 als d een kwadraat modulo 8, dus een 8-voud plus 1 is, anders $\chi$ (d, x) = -1 (en d is 8-voud plus 5);

3. x is niet priem, dan is $\chi$ (d, x) gelijk aan het product van de waarden $\chi$ (d, p) voor alle priemfactoren p van x, in het bijzonder ook $\chi$ (d, 1) = 1 (leeg product);

Kwadratische reciprociteit
Met behulp van van *kwadratische reciprociteit* - een forrmule bewezen door C.F. Gauss in 1796 (zie genoemde literatuur) – kunnen omkeringsformules worden afgeleid.

Discriminant d is ofwel 4-voud plus 1, ofwel 4-voud. Is d een 4-voud plus 1, dan is d te schrijven als product van oneven factoren $\pm$p, waarbij p de priemfactoren van d zijn en voor elke p het teken $\pm$ zo gekozen wordt dat $\pm$p een 4-voud plus 1 is.
Voor deze factoren geldt de omkeringsformule:

$\chi$ ($\pm$p, x) = 1 als x een kwadraat is modulo p, anders $\chi$ ($\pm$p, x) = -1.

Is d een 4-voud, dan is d een 4-voud plus 1 maal de even factor e = -4 of -8 of +8.
Voor deze factor e en x in de periode $0 \leq x < |e|$ geldt, met notatie: o = 0, + = +1, - = -1:

$\chi$ (-4, x) = o + o - , $\chi$ (-8, x) = o + o + o – o - , $\chi$ (8, x) = o + o – o – o + .

Bovendien geldt voor een discriminant d die product is van discriminanten a en b:

$\chi$ (d, x) = $\chi$ (a, x) maal $\chi$ (b, x) {multiplicativiteit voor factoren van d),

alsmede:

$\chi$ (d, x) = $\chi$ (d, x + |d|) {periodiciteit, periode |d|}.

Normen van priemgetallen en priemidealen
Voor de normen, n, van algebraische getallen en van idealen in een kwadratische ring geldt:

$\chi$ (d, n) = 0 of 1.

Is norm n priem, dan is n norm van een priemgetal (en dus ook van het hoofdideaal dat erdoor wordt voortgebracht). Is norm n het kwadraat van een priemgetal p, dan doet zich een van de volgende gevallen voor:

$\chi$ d, p) = -1: dan is p een priemgetal in de ring en hoofdideaal (p) een priemideaal;

$\chi$ (d, p) = 0 of 1:

dan is p product van twee priemgetallen met norm p of kan in een niet-UFD eventueel ondeelbaar zijn, maar niet priem; bovendien is het hoofdideaal (p) het product van twee priemidealen die elk norm p hebben. Is in het bijzonder $\chi$ (d, p) = 0, dan is p product van twee priemgetallen waarbij de ene gelijk is aan een eenheid maal de andere, en het hoofdideaal (p) is gelijk aan het product van een priemideaal P met zichzelf.

## 6. Algoritmen

Op grond van bovenstaande theorie kunnen algoritmen worden gegeven voor het berekenen van kwadratische karaakters en van (normen van) priemgetallen en priemidealen in kwadratische ringen.

Berekening van kwadratisch karakter
Zoals gesteld, is het karakter $\chi$ (d, n) periodiek in n met periode |d|. We hoeven het karakter dus slechts voor één periode te berekenen en deze door verschuiving over veelvouden ervan voort te zetten. Onderdelen van deze algoritme zijn bekend, zie bijv. Cohen (1993) 1.4.

Voor gegeven (al of niet kwadraatvrije) radicand wordt het karakter berekend als volgt.
De radicand wordt ontbonden in priemfactoren en eventuele kwadraten worden eruit gedeeld zodat een kwadraatvrije radicand r (met onderling verschillende priemfactoren) overblijft.
Hieruit wordt de bijbehorende discriminant d (= r of 4r) bepaald.
Vervolgens wordt voor elke oneven priemfactor p van d het karakter $\chi$ ($\pm$p, x) over een periode p bepaald als boven aangegeven. Als d een 4-voud is, dan komt er voor de even factor e = –4 of –8 of +8 nog het karakter $\chi$ (e, x) bij als boven aangegeven..

Het karakter van d wordt tenslotte verkregen door de karakters voor alle genoemde oneven priemfactoren en de eventuele factor e te vermenigvuldigen volgens de multiplicatieve eigenschap voor factoren van d.

Berekening van normen van priemgetallen en priemidealen
Deze algoritme hebben wij eerder gepubliceerd in Dekker (1994 & 2010).
We bepalen voor een ring met discriminant d een verzameling S = S(d, max) die alle normen niet groter dan max van priemidealen in de ring omvat als volgt.
Zoals gesteld, geldt voor deze normen $\chi$ (d, n) = 0 of 1.
Als $\chi$ (d, n) = 0 en n norm van een priemideaal is, dan zijn de enige mogelijke waarden van n de priemfactoren van d. We nemen dus eerst de priemfactoren van d in S op.
Verder nemen we in S op de getallen n tot aan max waarvoor $\chi$ (d, n) = 1.
Uitgaande van deze verzameling S wordt door middel van een zeefproces – analoog aan de zeef van Eratosthenes voor het berekenen van natuurlijke priemgetallen – alle veelvouden van andere elementen van S uit de verzameling verwijderd.
We krijgen dan een verzameling, T, bestaande uit:

1. alle priemgetallen p waarvoor $\chi$ (d, p) = 0 of 1;
2. alle kwadraten van priemgetallen p waarvoor $\chi$ (d, p) = -1;
3. alle producten pq van ongelijke priemen p en q waarvoor $\chi$ (d, p) = $\chi$ (d, q) = -1.

Deze laatste deelverzameling is overbodig maar kan geen kwaad, want deze getallen pq zijn geen mogelijke norm van priemidealen in de ring.
Vervolgens gebruiken we deze verzameling T voor het tekenen van plaatjes van priemgetallen, en eventueel ook priemidealen, in de kwadratische ring met discriminant d.

Nevenidealen

Nevenidealen (niet-hoofdidealen) kunnen worden verkregen door hoofdidealen te delen door een bepaald nevenideaal N, dat we kiezen zo dat zijn norm 'bynorm' een priemgetal is.
N is dan te schrijven als (bynorm, shift + $\tau$), waarbij bynorm en shift + $\tau$ het ideaal voortbrengen. Hierbij moet shift zo zijn dat bynorm deler is van de norm van shift + $\tau$.
De priem-nevenidealen worden dan voorgesteld door de getallen waarvan de norm gelijk is aan bynorm maal een priemgetal. Voor klassegetal groter dan 2 zijn N en shift nodig om onderscheid te maken tussen verschillende geconjugeerde klassen van nevenidealen.

In het bijzonder beschouwen we lichamen met klassegetal 2 en 3. Voor klassegetal 2 zijn er de volgende complexe lichamen en o.a. de volgende reële lichamen:

| r mod 4 | complex, r < 0 | reeël, r > 0 |
|---|---|---|
| 1 | -15 -35 -51 -91 -115 -123 –187 -235 -267 -403 -427 | 65 85 |
| 2 of 3 | -5 -6 -10 -13 -22 -37 -58 | 10 15 |

Voor klassegetal 3 zijn er alleen complexe lichamen met radicand congruent 1 modulo 4, namelijk de volgende 16:

-23 -31 -59 -83 -107 -139 –211 -283 -307 -331 -379 -499 -547 -643 -803 -907

en o.a de volgende reële lichamen: (r mod 4 = 2 of 3) 79, 142, (r mod 4 = 1) 229, 257.
Voor tabellen en informatie zie Borewicz & Safarevic(1966) en Cohen(1993).

Programma's

Onze algoritmen zijn geïmplementeerd in C (sub-) programma's voor het berekenen van kwadratische karakters en priemnormen, en voor het tekenen van plaatjes van priemgetallen, en eventueel priem-nevenidealen.
De programma's zijn geïmplementeerd in Xcode Developer voor Mac OS X.

Appendix: plaatjes

In Appendix presenteren we een selectie van plaatjes van priemgetallen in de ring van algebraisch gehele getallen voor kwadratische lichamen met klassegetal 1 (UFD), 2 en 3.
Boven elk plaatje wordt vermeld welk lichaam / ring het betreft, het klassegetal en het bijbehorende karakter 'chi' (voor zover de ruimte op de regel toelaat).
In de plaatjes staan gehele getallen op de x-as en gehele getallen maal $\sqrt{r}$ op de y-as.
De coördinaten x en y lopen van -47 tot +47. Maar voor radicand $\equiv$ 1 modulo 4 en y oneven doorloopt x de waarden geheel getal plus ½, zodat een driehoekig rooster ontstaat.
Op de laatste pagina vertonen we, voor niet-UFD, plaatjes van priemgetallen en priem-nevenidealen (deze in aparte kleur / kleuren). Hierbij worden bovendien de voor de nevenidealen benodigde parameters 'bynorm' en bij klassegetal 3 'shift' bovenaan vermeld.

Op elke pagina staan zes plaatjes. Op onze website https://staff.fnwi.uva.nl/t.j.dekker vertonen we een uitgebreidere collectie plaatjes.

Doel

Het doel is de fraaie patronen van de priemgetallen (en priem-nevenidealen) zichtbaar te maken. Voor zover de auteur weet zijn dergelijke plaatjes door anderen nooit vertoond, met uitzondering van die voor de bekende ring van Gauss $Z[\sqrt{-1}]$ en de ring $Z[(1+\sqrt{-3})/2]$, zie Van der Pol & Speziali (1951).

**Dank**

De schrijver betuigt zijn dank aan Hendrik W. Lenstra jr, Peter Stevenhagen en Herman J. J. te Riele voor stimulerende discussies en waardevolle opmerkingen over dit onderzoek.

**Literatuur**

S. I. Borewicz & I. R. Safarevic, Zahlentheorie (aus dem Russischen übersetzt von H. Koch); Birkhäuser Verlag, Basel (1966).
H. Cohen, A course in computational algebraic number theory; Springer-Verlag (1993).
T. J. Dekker, Prime numbers in quadratic fields, CWI Quarterly 7 (1994) 367-394.
T. J. Dekker: Primes in quadratic fields; arXiv:1001.5214 [math.NT] (2010).
K. Ireland & M. Rosen, A classical introduction to modern number theory; Springer Verlag, New York (1982).
P. G. Lejeune Dirichlet, Vorlesungen über Zahlentheorie, herausgegeben von R. Dedekind, 4. Auflage, Vieweg, Braunschweig (1893), reprint: Chelsea, New York (1968).
P. Levrie & R. Penne, De pracht van priemgetallen; Prometheus–Bert Bakker, Amsterdam (2014).
B. van der Pol & P. Speziali, The primes in k(ρ), Indag. Mathematicae XIII (1951) 9-15.
H. M. Stark, A complete determination of the complex quadratic fields of class-number one; Michigan Math. J. 14 (1967), 1 - 27.